REMARKS/ARGUMENTS

Claims 1-67 are currently pending in this application. Claims 1, 4, 9-10, 14, 21-22, 25, 30-31, 40, 42, 44-67 have been amended. The amendments find full support in the original specification, claims, and drawings. No new matter has been added. In view of the above amendments and remarks that follow, reexamination, reconsideration, and an early indication of allowance of claims 1-67 is respectfully requested.

Claims 1-3, 5-12, 15, 17-24, 26-33, 35-40, 43-46, 48-49, 51-52, 55-58, 60-61, and 63-64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (U.S. Patent No. 6,769,063) in view of Callum (U.S. Patent No. 6,320,964). Claims 4, 13-14, 25, 41-42, 47, 53-54, 59 and 65-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum and further in view of Steinman et al. (U.S. Patent No. 6,591,349). Claims 16, 34, 50, and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum and Steinman, and in further view of Teppler (U.S. Patent No. 6,792,536). Applicant respectfully traverses these rejections.

With respect to independent claims 1, 22, 44, and 56, the Examiner acknowledges that Kanda does not disclose, among other things, a "multiplexer circuitry having an input and output stage." However, the Examiner relies on Callum to make up for this deficiency.

Callum discloses a cryptographic accelerator with a selector 330, which, according to the Examiner, corresponds to the recited multiplexer circuitry, and a plurality of buses 310 coupled to the selector. (See, FIG. 3). The buses rearrange

the bit representation of an incoming data block during transmission to the selector. "Whichever cryptographic operation is chosen by select signal lines 360, the resulting data is produced and output from cryptographic accelerator 230 upon assertion of a read strobe (RS#) signal on signal line 370." (Col. 4, lines 1-7; FIG. 3).

Independent claims 1, 22, 44, and 56 have now been amended to recite a "cryptography engine" or "integrated circuit layout associated with a cryptography engine" that includes "first and second registers coupled to the output stage of the multiplexer circuitry, wherein the multiplexer circuitry selects between the first and second registers and provides the output of the expansion logic to a selected register for storing therein." (Emphasis added). Callum fails to teach or suggest such a "cryptography engine" or "integrated circuit layout." As discussed above, the selector circuitry disclosed in Callum simply outputs data produced by the cryptographic accelerator based on the cryptographic operation chosen by the select signals lines provided to the selector. Callum's selector does not, however, select "between the first and second registers" and further fails to provide "the output of the expansion logic to a selected register for storing therein" as is now required by the independent claims 1, 22, 44, and 56. Accordingly, claims 1, 22, 44, and 56 are now in condition for allowance.

Claims 2-21, 23-43, 45-55, and 57-67 are also in condition for allowance because they depend on an allowable base claim, and for the additional limitations that they contain.

Appln No. 09/892,310
Amdt date December 30, 2004
Reply to Office action of September 30, 2004

In view of the above amendments and remarks, Applicant respectfully requests reexamination, reconsideration, and an early indication of allowance of claims 1-67.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By
Josephine E. Chang
Reg. No. 46,083
626/795-9900

JEC/lal
JEC PAS591073.1-*-12/30/04 4:52 PM